CHAPTER 129
FORMERLY
HOUSE SUBSTITUTE NO. 1
TO HOUSE BILL NO. 180
AS AMENDED BY
HOUSE AMENDMENT NO. 3 AND
SENATE AMENDMENT NO. 1

AN ACT TO AMEND TITLE 6 OF THE DELAWARE CODE RELATING TO BREACHES OF SECURITY INVOLVING PERSONAL INFORMATION.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF DELAWARE:

Section 1. Amend Chapter 12B, Title 6 of the Delaware Code as follows and redesignating accordingly:

§ 12B-100. Protection of personal information.

Any person who conducts business in this State and owns, licenses, or maintains personal information shall implement and maintain reasonable procedures and practices to prevent the unauthorized acquisition, use, modification, disclosure, or destruction of personal information collected or maintained in the regular course of business.

§ 12B-101. Definitions.

For purposes of this chapter:

(1) "Breach of security" means as follows:

a. The unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information. Good faith acquisition of personal information by an employee or agent of any person for the purposes of such person is not a breach of security, provided that the personal information is not used for an unauthorized purpose or subject to further unauthorized disclosure.

b. The unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information is not a breach of security to the extent that personal information contained therein is encrypted, unless such unauthorized acquisition includes, or is reasonably believed to include, the encryption key and the person that owns or licenses the encrypted information has a reasonable belief that the encryption key could render that personal information readable or useable.

(2) [Repealed.]

( ) "Determination of the breach of security" means the point in time at which a person who owns, licenses, or maintains computerized data has sufficient evidence to conclude that a breach of security of such computerized data has taken place.

( ) "Encrypted" means personal information that is rendered unusable, unreadable, or indecipherable through a security technology or methodology generally accepted in the field of information security.

( ) “Encryption key” means the confidential key or process designed to render the encrypted personal information useable, readable, and decipherable.

(3) "Notice" means any of the following:

a. Written notice.

b. Telephonic notice.

c. Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in § 7001 of Title 15 of the United States Code or if the person’s primary means of communication with the resident is by electronic means.

d. Substitute notice, if the person required to provide notice under this chapter demonstrates that the cost of providing notice will exceed $75,000, or that the affected number of Delaware residents to be notified exceeds 100,000 residents, or that the person does not have sufficient contact information to provide notice. Substitute notice consists of all of the following:

1. Electronic notice if the person has email addresses for the members of the affected class of Delaware residents.

2. Conspicuous posting of the notice on the web site page of the person if the person maintains one.

3. Notice to major statewide media, including newspapers, radio, and television and publication on the major social media platforms of the person providing notice.

( ) “Person” means an individual; corporation; business trust; estate trust; partnership; limited liability company; association; joint venture; government; governmental subdivision, agency, or instrumentality; public corporation; or any other legal or commercial entity.

(4)a. "Personal information" means a Delaware resident's first name or first initial and last name in combination with any 1 or more of the following data elements that relate to that individual:

1. Social Security number.

2. Driver's license number or state or federal identification card number.

3. Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account.

4. Passport number.

5. A username or email address, in combination with a password or security question and answer that would permit access to an online account.

6. Medical history, medical treatment by a healthcare professional, diagnosis of mental or physical condition by a health care professional, or deoxyribonucleic acid profile.

7. Health insurance policy number, subscriber identification number, or any other unique identifier used by a health insurer to identify the person..

8. Unique biometric data generated from measurements or analysis of human body characteristics for authentication purposes.

9. An individual taxpayer identification number.

b. “Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely-distributed media.

§ 12B-102. Disclosure of breach of security; notice.

(a) Any person who conducts business in this State and who owns or licenses computerized data that includes personal information shall provide notice of any breach of security following determination of the breach of security to any resident of this State whose personal information was breached or is reasonably believed to have been breached, unless, after an appropriate investigation, the person reasonably determines that the breach of security is unlikely to result in harm to the individuals whose personal information has been breached.

(b) A person that maintains computerized data that includes personal information that the person does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of security immediately following determination of the breach of security. For purposes of this subsection, “cooperation” includes sharing with the owner or licensee information relevant to the breach.

(c) Notice required by § 12B-102(a) of this title must be made without unreasonable delay but not later than 60 days after determination of the breach of security, except in the following situations:

(1) A shorter time is required under federal law.

(2) A law enforcement agency determines that the notice will impede a criminal investigation and such law enforcement agency has made a request of the person that the notice be delayed. Any such delayed notice must be made after such law enforcement agency determines that notice will not compromise the criminal investigation and so notifies the person of such determination.

(3) When a person otherwise required by § 12B-102(a) of this title to provide notice, could not, through reasonable diligence, identify within 60 days that the personal information of certain residents of this State was included in a breach of security, such person must provide the notice required by § 12B-102(a) of this title to such residents as soon as practicable after the determination that the breach of security included the personal information of such residents, unless such person provides or has provided substitute notice in accordance with § 12B-101(3)d. of this title.

(d) If the affected number of Delaware residents to be notified exceeds 500 residents, the person required to provide notice shall, not later than the time when notice is provided to the resident, also provide notice of the breach of security to the Attorney General.

(e) If the breach of security includes a social security number, the person shall offer to each resident, whose personal information, including social security number, was breached or is reasonably believed to have been breached, credit monitoring services at no cost to such resident for a period of 1 year. Such person shall provide all information necessary for such resident to enroll in such services and shall include information on how such resident

can place a credit freeze on such resident's credit file. Such services are not required if, after an appropriate investigation, the person reasonably determines that the breach of security is unlikely to result in harm to the individuals whose personal information has been breached.

(f) In the case of a breach of security involving personal information defined in § 12B-101(4)a.6. of this title for login credentials of an email account furnished by the person, the person cannot comply with this section by providing the security breach notification to such email address, but may instead comply with this section by providing notice by another method described in § 12B-101(3) of this title or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the person knows the resident customarily accesses the account.

§ 12B-103. Procedures deemed in compliance with security breach notice requirements.

(a) Under this chapter, a person that maintains its own notice procedures as part of an information security policy for the treatment of personal information, and whose procedures are otherwise consistent with the timing requirements of this chapter is deemed to be in compliance with the notice requirements of this chapter if the person notifies affected Delaware residents in accordance with its policies in the event of a breach of security.

(b) Under this chapter, a person that is regulated by state or federal law, including the Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191, as amended) and the Gramm Leach Bliley Act (15 U.S.C. § 6801 et seq., as amended) and that maintains procedures for a breach of security pursuant to the laws, rules, regulations, guidance, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with this chapter if the person notifies affected Delaware residents in accordance with the maintained procedures when a breach of security occurs.

§ 12B-104. Violations.

(a) Pursuant to the enforcement duties and powers of the Director of Consumer Protection of the Department of Justice under Chapter 25 of Title 29, the Attorney General may bring an action in law or equity to address the violations of this chapter and for other relief that may be appropriate to ensure proper compliance with this chapter or to recover direct economic damages resulting from a violation, or both. The provisions of this chapter are not exclusive and do not relieve a person subject to this chapter from compliance with all other applicable provisions of law.

(b) Nothing in this chapter may be construed to modify any right which a person may have at common law, by statute, or otherwise.

Section 2. This Act shall become effective 240 days after its enactment into law.

Approved August 17, 2017